Elektron dövlətdə veb xidmətlərinin təhlükəsizliyinin qiymətləndirilməsi

Tural Yunusov
AMEA İnformasiya Texnologiyaları İnstitutu
turaly@mail.ru

***Xülasə*— Məqalədə e-dövlətin veb xidmətlərinin təhlükəsizliyinin qiymətləndirilməsi, e-xidmətlərə mövcud təhdidlərin analizi, e-xidmət təhlükəsizliyi üçün vahid model və e-xidmət təhlükəsizliyi üçün ümumi təhdidlər qiymətləndirilmişdir.**

***Açar sözlər* - e-dövlət, informasiya təhlükəsizliyi, təhlükəsizliyin qiymətləndirilməsi, təhdidlərin analizi**

I. GİRİŞ

Veb-texnologiyaların böyük sürətlə inkişafı və qlobal informasiya fəzasının bütün istiqamətlərini əhatə etməsi veb-texnologiyaların təhlükəsizliyini nə qədər vacib məsələyə çevirmişdir. Hazırda e-dövlət mühitində, biznes dünyasında və vətəndaş cəmiyyətində tərəflərin informasiya qarşılıqlı təsiri əsasən veb-texnologiyalar vasitəsilə həyata keçirilir.

Dünya ölkələrinin çoxunda e-dövlət vətəndaşlara və biznes sektoruna veb xidmətlər vasitəsilə xidmət göstərir. Bir sıra qiymətləndirmə metodologiyalarında e-dövlətin inkişaf mərhələləri bilavasitə veb-texnologiyalardan istifadə səviyyəsi ilə müəyyən edilir [1].

Veb-texnologiyalarının inkişafı, xüsusilə sosial şəbəkələrin sürətlə yayılması və veb-texnologiyaları üzrə yeni tətbiqlərin artması, ödənişlərin internet üzərindən internet-bankinq vasitəsilə ödənilməsi, internet mağazalar çox geniş şəkildə istifadə olunması e-dövlət veb xidmətləri təhlükəsizliyini və təhlükəsizliyin qiymətləndirilməsini mühüm məsələlərdən birinə çevirir.

Yerli özünüidarəetmə orqanlarında informasiya texnologiyalarının (İT) geniş tətbiqi və inkişaf etdirilməsi informasiya cəmiyyətinin formalaşmasında mühüm mərhələ olan e-dövlətin qurulmasına şərait yaradır. Təhsil prosesində və elmi fəaliyyətdə elektron kitabxanalar və distant təhsil formaları istifadə edilir. İnternetin inkişafı xüsusi “virtual mədəniyyətin” meydana çıxmasına şərait yaradır. İnformasiya texnologiyalarının iqtisadi münasibətlərdə geniş istifadəsi nəticəsində “şəbəkə” iqtisadiyyatı formalaşır, “elektron pullar”, “elektron ticarət” meydana çıxır. Yeni şəraitdə hüquqi münasibətlərin tənzimlənməsi üçün “informasiya hüququ” formalaşır. İnformasiya cəmiyyətinə keçid üçün əlverişli şəraitin yaradılmasında dövlət aparıcı rol oynayır və bu keçid prosesində dövlətin özü də e-dövlətə çevrilir. Son onillikdə dünyanın bir çox ölkəsində e-dövlətə keçid üzrə bir sıra milli və beynəlxalq proqramlar həyata keçirilməkdədir [2].

II. E-DÖVLƏT VEB XİDMƏTLƏRİNİN TƏHLÜKƏSİZLİYİNİN QİYMƏTLƏNDİRİLMƏSİ

E-xidmət müştərilərin, vətəndaşların və korporasiyaların xidmət təminatçıları ilə informasiya aktivlərinin və resurslarının dəstəkləndiyi köməkçi infrastrukturundan istifadə edərək internet vasitəsilə qarşılıqlı əlaqəyə girməsinə imkan yaradır. İnformasiya aktivləri və resursları hər bir yeni təhdidə qarşı zəif olduqları üçün risk mənbəyinə çevriliblər [3]. E–xidmətlər üzrə təhdidlər istənilən informasiya texnologiyalarının təhdidləri ilə eynidir və aşağıdakı kimi təsnif edilə bilər:

- Təbii sürətdə yaranan təhdidlər, məsələn daşqın və ya zəlzələ kimi gözlənilməz hadisələrin daxil olduğu “Təbii hadisələr” və ya “Fors-major” kimi terminlərlə ifadə olunur.
- Plan və ya prosedurda çatışmayan amillərin səbəb olduğu hallar zamanı yaranan qəza təhlükələri.
- Maliyyə vəsaitlərini köçürmək məqsədilə məlumatın silinməsi kimi əməliyyatlara cəlb olunan heyətin birbaşa və ya bilavasitə səbəb olduğu məqsədli təhlükələr [4].

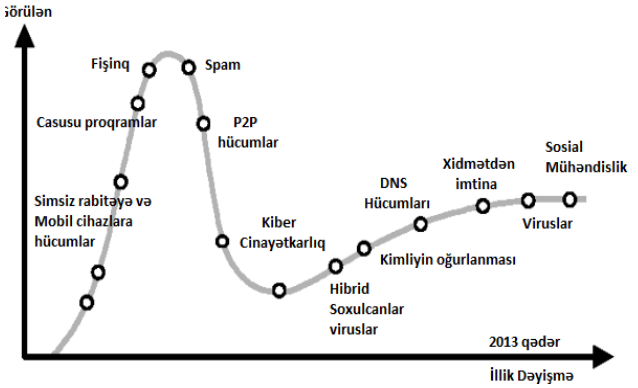
Müəssisələr özlərinin informasiya sistemlərinin təhlükəsizliyini yalnız müxtəlif texniki üsulların vasitəsilə həll etməyə çalışırlar. İdarəetməyə nəzarət mexanizmləri və ya istənilən insan amilinin səbəb ola biləcəyi potensial böhranlara əhəmiyyət verməmək onlayn xidmətlər üzərində təhdid səviyyəsini artırır. [5]-də aktivlərin növünə əsasən informasiya sistemlərinə olan təhdidlərin təsnifatı aparılmışdır. İnformasiya təhdidləri üçün 7 kateqoriya müəyyən edilmişdir və hər bir kateqoriyanın müxtəlif funksiyaları vardır:

- Proqram təminatı.
- Texniki avadanlıq.
- Məlumat bazası.
- Şəbəkə.
- Fiziki.
- İşçi heyət.
- İdarəetmə.

E-xidmət sadəcə xidmət təminatçısına məxsus olan İT infrastrukturunun və ya üçüncü şəxslər vasitəsilə kənar mənbəyin məhsuludur. E-xidmətə yardımçı texnologiya, vahid proseslər və yardımçı heyət daxildir. Onlayn xidmətin istənilən əsas elementləri üzrə təhlükəsizliyin pozulması problemi xidmət və onun istifadəçiləri üçün birbaşa təhdid yaradır.

İnternetin geniş yayılması ilə yanaşı, təhdidlərin artması halı da davam edir. Aşağıdakı diaqramda müəyyən edilmiş bəzi təhdidlər və növbəti illərdə onların artım dinamikası

göstərilmişdir (şəkil 1). Gartner təşkilatı fişinq, reklamları avtomatik yükləyən proqramları, gizli məlumatları oğurlayan proqramları və kimliyin oğurlanmasını əsas təhlükə mənbəyi kimi qiymətləndirir [6]. Təhdidlərin artması onu göstərir ki, gələcəkdə daha çox təhdidlə üzləşəcəyik. Təhdidlərin yarada biləcəyi ziyanı azaltmaq məqsədilə təhlükəsizlik üçün müxtəlif əks tədbirlərə ehtiyac vardır. Bu əks tədbirlərin xarakteri texnoloji ola və ya texnoloji olmaya bilər.



Şəkil 1: Təhdidlərin illər üzrə artım dinamikası

Bir proqramın səbəb olduğu təhdidlər virus hücumlarından başlayaraq icazəsiz girişə qədər bir-birindən fərqlənir [7]. Burada e-xidmətlərin biznes proqramlarından yaranması faktını və hər bir proqram üçün çoxlu təhlükələr olduğunu nəzərə alaraq, çoxsəviyyəli təhlükəsizlik modeli konsepsiyası təklif edilir. [7]-də təhlil edilən proqramlar üzrə təhdidlər aşağıdakılardır:

- İstifadəçi girişində viruslu sql məlumat bazası.
- Daxil olma məlumatının açıqlanması.
- Əməliyyat zamanı kimliyin oğurlanması.
- İstifadəçi məlumatlarının açıqlanması.
- Məlumat bazasına birbaşa icazə.
- E-poçt bildirişinin blok edilməsi.
- İstifadəçinin məlumatlarına müdaxilə.
- Yeni sorğu bildirişinin blok edilməsi.
- Hesabın silinməsi.
- Veb səhifənin dağılması.
- Şəxs haqqında etibarlı məlumat olmadan sayta daxil olma.

Yuxarıda qeyd olunan təhdidlər proqramın idarə edilməsinin texnoloji tərəfi üzrə təhlükələri əks etdirir [7]. E-xidmət ardıcıl avtomatlaşdırılmış proses vasitəsilə təmin edilir və ya bu birbaşa insan müdaxiləsinə ehtiyac duyulan əl ilə idarə olunan prosedur vasitəsilə dayandırılan prosesin avtomatlaşdırılmasıdır. E-xidmət üçün təhdid texnoloji qüsur, müvafiq təhlükəsizliyin çatışmazlığı, təhdidlərlə mübarizə aparmaq üçün təhlükəsizliyin pozulması haqqında lazımi miqdarda məlumatın olmaması, aydın və ciddi olmayan operativ prosedur və ya xidməti işə salmaq üçün yanlış zamanın seçilməsi nəticəsində yarana bilər. Bununla razılaşmaq olar ki, əgər təhlükə texnologiya, kompetensiya, siyasət, müvafiq şəkildə idarəetmənin olmaması və yanlış qərarların birləşməsi nəticəsində baş verərsə, istənilən e-xidmət üzrə təhlükənin ciddiliyi həmişə daha da yüksək olacaq.

Düstur 1-dən görüldüyü kimi təhdid cinayətkarın bacarığı ilə onun fəaliyyət məqsədinin birləşməsidir.

$$Təhdid = Bacarıq + Məqsəd \quad (1)$$

$$Bacarıq = Daxil\ olma + Ustalıq \quad (2)$$

Bacarıq elementi İT heyətin və ya infrastruktur üçün məsuliyyətli olan təhlükəsizlik işçilərinin kompetensiya dərəcəsi ilə birbaşa əlaqədardır. Təhdid riskin daha məhdud komponentidir [8]. Təhlükəsizlik üzrə bəzi analitiklər təhdidləri informasiya və ya informasiya sisteminə potensial risk kimi izah edirlər [9, 10]. Təhdidlər riyazi olaraq, onun komponentlərini hesablaya bildiyimiz təqdirdə, yuxarıdakı düsturlarda təsvir olunduğu kimi hesablana bilər. İlkin mərhələdə e-xidmət üzrə baş verə biləcək təhlükələri nəzərə almaq təhdidlərə qarşı zəifliklərin təsirini azaldacaq. Bundan əlavə, yuxarıdakı düsturlarda göstərildiyi kimi güclü təhlükəsizlik kompetensiyasının olması düstur 1 – dəki təhdidin dəyərini azaldaraq hücum edənin bacarığını minimum həddə çatdıracaq. Həm güclü təhlükəsizlik kompetensiyasının, həm də texnologiyaların olması bacarıq dəyərini (düstur 2) daha da azaldacaq və bu səbəbdən də, o təhdidin dəyərini azaltmış olacaq.

Riskin dərəcəsini hesablamağın standart üsulu təhdidin dərəcəsini zəifliyin mühümlüyünə vuraraq infrastrukturu mühafizə etmək üçün mövcud olan əks tədbirlərin səviyyəsinə bölmək və onu təsirə vurmaqdır (düstur 3). Bu üsul aktivlər üzrə zəifliklər və təsirlərdən xəbərdar olmaqdan çox asılıdır. Bu bizim zəifliklər üzrə yenilənmiş biliyimizə və təsirin müxtəlif növlərini tədqiq etmək üzrə təcrübəmizə əsaslanır. Aşağıda göstərilən düsturlar riski hesablamağın standart üsulunu əks etdirir [11].

$$Riskin\ dərəcəsi=((Təhdid\ Zəiflik)/Əks\ tədbirlər)\ Təsir \quad (3)$$

$$Ümumi\ Risk=Zəiflik+Təhdidlər+Aktivlərin\ Dəyəri \quad (4)$$

III. E-XİDMƏTLƏRİN TƏHLÜKƏSİZLİYİ ÜÇÜN VAHİD MODEL ANALİZİ

Elmi tədqiqatların analizi göstərir ki, e-dövlət tərəfindən təklif olunan e-xidmətlərə olan təhdidləri təhlil etməyə xidmət edən vahid yanaşma təklif edilməmişdir. Tədqiq edilən sənədlərin əksəriyyəti infrastrukturun mühafizəsi vasitəsi ilə e-dövlətin problemləri göstərilmişdir [12]. Heç bir şübhə yoxdur ki, infrastrukturun mühafizəsinə yanaşma e-xidmətlər üçün bəzi riskləri yüngülləşdirəcək, ancaq bütün təhdidlərin qarşısını almaq üçün bu kifayət deyil. E-xidmətlər həmişə ardıcıl tam avtomatlaşdırılmış proseslərlə dəstəklənmir və ya ümumi texnoloji infrastruktur ilə təklif edilmir. Təhlükəsizlik siyasətləri və prosedurları təklif olunan bütün e-xidmətlər üçün ümumi olmaya bilər və dəstək heyəti müxtəlif dərəcəli kompetensiyalara malik ola bilər. Bundan əlavə, təklif olunmuş yanaşmaların əksəriyyəti fiziki və şəbəkə təhlükəsizliyi daxil olmaqla xidməti mühafizə sistemlərinin müxtəlif növləri üzrə təhdidlərin təsirini nəzərə almışdır. E-xidmətlər bir və ya bir

neçə biznes proqramları ilə təmin edilə bilər. E-xidmətin işə salınması prosesi texnologiyanın etibarlılığı, e-xidmətlə əlaqədar xüsusi təhlükəsizlik siyasətləri inkişaf etdirmək ehtiyacı və müvafiq dəstək heyətinin və əməliyyat prosedurlarının mövcudluğundan yüksək səviyyədə asılı ola bilər. Aşağıdakılar e-xidmətlər üçün tələb olunan mühüm təhlükəsizlik səviyyələridir.

Təhlükəsizliyin texniki infrastrukturu

Təhlükəsizlik texnologiyalarının e-xidmətləri dəstəkləyən sistemləri və proqramları mühafizə etməkdə mühüm rolu vardır. Müdaxilələrin aşkarlanması sistemləri, antiviruslar [13], kriptoqrafiya [14], virtual xüsusi şəbəkə [15], rəqəmsal imza [16] və təhlükəsizlik protokolu [17] kimi texnologiyalar istifadəçilərin böyük inamını təmin etməklə e-xidmətlərin müvəffəqiyyətinə imkan yaradır. Təhlükəsizlik tədbirlərinin hamısının və ya bəzilərinin olmaması ümumi təhlükəsizliyə mənfi təsir edəcəkdir və e-xidmət üçün təhdid hesab edilə bilər.

E-xidmətlə əlaqədar təhlükəsizlik siyasəti

Təhlükəsizlik siyasətləri istənilən təşkilatın təhlükəsizlik sistemində bir mərhələdir. Təhlükəsizlik siyasəti təşkilata məxsus spesifik qanundur. Bu işçilərə hansı fəaliyyətlərin həyata keçirilməsinə icazə verilməsi və təşkilatın qayda və əsasnamələrinə əsasən hansı hərəkətin düzgün olmayan davranış hesab edildiyini bilməyə imkan yaradır [18]. Güclü təhlükəsizlik siyasətinin mövcud olması daxili təhdidləri azaltmaqda elektron əsaslı təşkilata köməklik göstərir [19, 20]. İstənilən təşkilatda yerinə yetirilə bilən təhlükəsizlik siyasətlərinin bir neçə növü vardır. Təşkilat sistemin təhlükəsizlik siyasəti, məhsulun təhlükəsizliyi siyasəti, icmanın təhlükəsizliyi siyasəti və korporativ informasiyanın təhlükəsizliyi siyasətini həyata keçirə bilər [21]. Müvafiq təhlükəsizlik siyasətlərinin çatışmazlığı və ya onların tətbiqi e-xidmətlər üçün təhdid hesab edilə bilər. Təhlükəsizlik siyasətinin sənədi müxtəlif funksiyalarla əlaqədar siyasətlər toplusundan hazırlandığı üçün, alt siyasətin çatışmazlığı e-xidmətin ümumi təhlükəsizliyinə təhdid hesab edilə bilər.

Səriştəli təhlükəsizlik komandası və əməkdaşları

Heyətin peşəkarlığı açıq şəkildə istənilən təhlükəsizlik sisteminin əsas tələbidir. Təhlükəsizlik proqramını idarə etmək və ya onu müdafiə etmək bilik səviyyəsi az olan heyət üzərində mütləq asılılığın olması ümumi təhlükəsizlik sistemini böyük risk altına qoyacaq [19, 22].

Təhlükəsiz istismar və idarəetmə prosedurları

Təhlükəsizliyin idarə edilməsi üsulu müvəffəqiyyətli təhlükəsizlik proqramı və uğursuz olanı arasında fərqi müəyyən edir. Güclü təhlükəsizlik proqramının baş verən hadisələrə qarşı reaksiya tədbirləri prosesi, operativ təhlükəsizlik proseduru və lazım olan bütün idarəetmə proqram vasitələri olacaq. Təhlükəsizlik proqramının istismarı və idarəetməsi mühafizəni, zəifliyi müəyyən etməni və cavab tədbirlərini əhatə etməlidir [23].

Qərar qəbul etmənin sistematik üsulu

Yuxarıda qeyd olunan bütün təhlükəsizlik səviyyələri e-xidmətin işə salınmasına müvəffəq olmaq və vətəndaşlar tərəfindən yararlılığını artırmaq üçün mühümdür. İşə salma vaxtı, işə salma üsulu və e-xidmətin məzmunu təlükəsizlik heyəti tərəfindən nəzərə alınmağa ehtiyacı olan amillərdir. E-xidmətin yanlış işə salınması və ya mühüm təhlükəsizlik kriteriyasının qarşılanmadığı zaman işə salınmasına icazə verilməsi e-xidmət üçün təhlükədir. Təhlükəsizlik tədbirlərinin prioritetlərinin müəyyən edilməsi e-xidmət üçün düzgün qərarın verilməsində əsasdır.

Cədvəl 1-də e-xidmətlərin təhlükəsizlik proqramının hər bir səviyyəsi (texnoloji, təhlükəsizlik siyasətləri, peşəkarlıq, istismar və idarəetmə prosedurları, qərarın təsiri) ilə əlaqədar təhdidlər toplusu olması ideyasını sadələşdirir. Təhdidlər sistem və ya siyasətdəki qüsurlar ilə əlaqəli ola bilər və ya zəif operativ təhlükəsizlik proseduru və təhlükəsizlik kompetensiyasına görə yarana bilər. İdarəetmə qərarının təsirini nəzərə alaraq, səhv qərarın verilməsi təhlükəsi də həmçinin nəzərə alınmışdır. Təhdidlərin sayı bir e-xidmətdən digərinə qədər dəyişir və təhlükəsizlik proqramı ilə əlaqədar səviyyələrin sayı da həmçinin arta bilər.

E-Dövlət Xidmətləri						
	Səhv qərarlardan yaranan təhdidlər (TE)	TE1				
	Operativ idarəetmə prosedura təhdidləri (TD)	TD1	TD2			
	Səlahiyyətli təhlükəsizlik işçisinin olmaması təhdidi (TC)	TC1	TC2	TC3		
	Ciddi təhlükəsizlik siyasətinin olmaması təhdidi (TB)	TB1	TB2	TB3	TB4	
	Texnologiya ilə əlaqədar boşluqlar (TA)	TA1	TA2	TA3	TA4	TA5

CƏDVƏL I. TƏHLÜKƏSIZLIYIN QIYMƏTLƏNDIRILMƏSINƏ ƏSAS YANAŞMALAR

Burada TE1–xidmət nə vaxt və necə başladılmışdır; TD1–operativ təhlükəsizlik prosedurları mövcud deyil; TD2–insidentə qarşı reaksiya prosedurası mövcud deyil; TC1–hücumlar haqqında köhnə biliklər; TC2–informasiyanın klasifikasiya edilməsi biliklərinin olmaması; TC3–incidentin idarə edilməsi biliklərinin olmaması; TB1–internet siyasətinin olmaması; TB2–şifrlərin idarə edilməsi və seçilməsi siyasətinin olmaması; TB3–xidmətlərin başladılması siyasətinin olmaması; TB4–informasiyanın idarə edilməsi siyasətinin olmaması; TA1–əməliyyat sistemi nöqsanları; TA2–viruslar; TA3–şəbəkələrarası ekranın düzgün işləməməsi; TA4–DDOS hücumlar; TA5–fişinq.

IV. ÜMUMİ TƏHDİDLƏRİN DƏYƏRLƏNDİRİLMƏSİ

Sadə bir şəkildə, ümumi təhdidlərin dəyəri e-xidmət üçün hər bir səviyyədə təhlükənin baş vermə ehtimalının yekunu hesab edilə bilər. Təhlükəsizlik tədbirləri bununla əlaqədar təhdidləri azaltmaq məqsədilə hər bir səviyyədə müəyyən edilməlidir. Düstur 4-ə əsasən, hər bir səviyyənin təhdid dəyəri aşağıdakı kimidir:

$$T(i)=T1+T2+T3+T4..Tn \quad (5)$$

Bunun isə aşağıda qeyd edildiyi kimi risk dərəcəsi düsturu və ümumi risk düsturu üzərində birbaşa təsiri olacaq:

$$Riskin\ dərəcəsi=((\sum_{i=1}^{n} T(i)\ Təhdid)/\ Əks\ tədbirlər) \quad (6)$$

$$Ümumi\ Risk=Zəiflik \sum_{i=1}^{n} T(i)\ TəhdidlərAktivlərin\ Dəyəri \quad (7)$$

V. NƏTİCƏ

E-dövlət veb xidmətlərinin təhlükəsizliyi binar xüsusiyyətə malik deyil. Onun qiymətləndirilməsi zamanı çoxlu sayda faktorlar nəzərə almaq lazımdır. E-dövlət veb xidmətlərinin təhlükəsizliyinin qiymətləndirilməsi üçün müfəssəl, dəqiq funksiyalar və ölçmələr bu gün də problem olaraq qalmaqdadır. E-dövlət veb xidmətlərinin təhlükəsizliyinin qiymətləndirilməsi sahəsində real irəliləyişə nail olmaq üçün problemlərin müəyyən edilməsi və eksperimental metodların, dəqiq təhlükəsizlik metrikalarının və modellərinin yaradılması zəruridir.

Məqalədə e-dövlət veb xidmətlərinin təhlükəsizliyinin qiymətləndirilməsinin bəzi metodları, o cümlədən təhlükəsizliyin texniki infrastrukturu, e-xidmətlə əlaqədar təhlükəsizlik siyasəti, təhlükəsiz istismar və idarəetmə proseduraları və mövcud problemlər müəyyən edilmişdir. Həmçinin e-dövlət veb xidmətlərinin təhlükəsizliyinin qiymətləndirilməsinə əsas yanaşmalar, qiymətləndirmə üsulları analiz edilmiş və e-xidmətlərə olan ümumi təhdidlər dəyərləndirilmişdir. Bu analizin nəticəsi e-dövlət veb xidmətlərinin təhlükəsizliyinin qiymətləndirilməsi və dəyərləndirilməsi sahəsində mövcud olan bəzi problemlərin həll edilməsinə imkan verəcək.

ƏDƏBİYYAT

[1] C .Baum, A. Di Maio, Gartners four phases of e-government model, 2000, 400p.

[2] The UN E-Government Survey 2008: from e-Government to connected governance, United Nations, 2007, 225p.

[3] R. K. Rainer, C. A Snyder,. and H. H. Carr "Risk analysis for information technology", Journal of Information Management Information Systems, 1991, vol. 8, no. 1, pp.129-147

[4] K. R. A. Lindup, "New Model for Information Security Policies", Proceedings of COMPSEC International 1995, 25-27 Oct. 1995, London, UK, SRI International, Oxford, UK, 1995, 352p.

[5] D. C Icove and K. Vonstorch, Computer Crime, A Crime fighter’s Handbook, O'Reilly and Associates, Inc, Sebastopol, 1999, 464p.

[6] N. Schroder, Forecast: Security Software, Worldwide,2005-2009, Gartner 2005, 282p.

[7] F. Swiderski, W.C Snyder, Threat Modelling, Microsoft Press, Redmond, Washington. 2004, 385p.

[8] J. K Tudor,. Information Security Architecture-An Integrated Approach to Security in the Organization, Auerbach. 2002, 425p.

[9] R. K Nichols, D. J. Ryan and J. J. C. Ryan, Defending your Digital Assets Against Hackers, Crackers, Spies & Thieves, 1st ed, McGraw-Hill, U.S, 2000, 652p.

[10] A. Tiwana, Are Firewalls Enough? Web Security, Digital Press, 1999. 120p.

[11] T. Finne, "A DSS for Information Security Analysis: Computer Support in a Company's Risk Management", Proceedings of IEEE International Conference on Systems, Man and Cybernetics, 1996, Vol. 1, 14-17 Oct.

[12] D. A Smith,. and Garton, Specifying specific deterrence, American Sociological Review, vol. 54,1999.

[13] B. Schneier, , Secrets and Lies, Digital Security in a Networked World, 1st ed, Wiley, US, 2004, 225p.

[14] B. Schneier, Practical Cryptography, 1st ed, Wiley, US, 2003, 595p.

[15] J. M. Carroll, Computer Security, 3rd ed, Butterworth-Heinemann, Burlington, MA, 1995, 366p.

[16] B. Schneier, , Managed Security Monitoring, Network Security for the 21st Century, Commuter Secur. J., 2001, vol. 17, no. 2, pp. 1-12.

[17] D. F. C.Brewer, and M. J Nash, Chinese Wall security policy, Security and Privacy, IEEE Symposium, 1-3 May 1989, Oakland, CA, USA, pp. 206-214.

[18] C. Wood, Security Policy Made Easy, 10th ed, Information Shield, U.S, 2005, 381p.

[19] S. Kesh, S. Ramanujan, and S. Nerur, A Framework for Analyzing e-commerce Security, Computer and Security, 2002, pp. 149-158.

[20] M. T Siponen,. Five Dimensions of Information Security Awareness, Computers and Society, 2001 vol. 31, no. 2, pp. 24-9.

[21] K. R. A Lindup,.New Model for Information Security Policies, Proceedings of COMPSEC International 1995 128p.

[22] M. Gottfredon, and T. Hirschi, A General Theory of Crime, Stanford University Press, Stanford California 1990, 415p

[23] L. A Zadeh,.Fuzzy Sets, Information Control, 2000, vol. 19-21, pp. 8, 338-353.